In the Claims:

Please amend claims 1-3 and 5-21. The claims are as follows:

1-3. (Canceled) A method of securely comparing a first document in possession of a first party and a second document in possession of a second party, without revealing the contents of the first document to the second party or the contents of the second document to the first party, said method comprising the steps of:

i) said first and second parties each generating its own set of random data;

ii) each party exchanging said set of random data and a shared hash function with the other party;

iii) each party computing a first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by that party's set of random data, followed by the other party's set of random data;

iv) each party computing a second value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by the other party's set of random data, followed by that party's set of random data;

v) each party sending its first value to the other party and receiving the other party's first value;

vi) each party comparing said other party's first value to its second value;

vii) each party concluding that if the said values are the same, then the two documents are the same, but that otherwise said two documents are different;

viii) after computing said first and second values according to steps iii) and iv) above, each said first and second parties sending confirmation to the other party that each said party's first and second values have been computed, and waiting for said confirmation from said other party that each said party's first and second values have been computed before proceeding;

ix) after one party has sent its first value to the other party according to step v) above, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time;

x) after step i) and before step ii), each party examining the other party's set of random data for suitability and aborting the comparison if suitability is not established,

wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data.

5-21. (Canceled)